



CVE-2017-0904

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2017-0904
State	PUBLIC
Assigner	support@hackerone.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-11-13 17:29:00 UTC
Updated	2019-10-09 23:21:00 UTC
Description	The private_address_check ruby gem before 0.4.0 is vulnerable to a bypass due to use of Ruby's Resolv.getaddresses me

Risk And Classification

Problem Types: CWE-755

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Private Address Check Project	Private Address Check	All	All	All	All
Application	Private Address Check Project	Private Address Check	All	All	All	All

References

Reference	Source	Link
Fix bypass bug with malformed addresses · jtdowney/private_address_check@58a0d7f · GitHub	CONFIRM	github.
HackerOne	MISC	hacker
Resolv::getaddresses bug allows one to bypass your SSRF filter. · Issue #1 · jtdowney/private_address_check · GitHub	CONFIRM	github.
EdOverflow - Bypassing Server-Side Request Forgery filters by abusing a bug in Ruby's native resolver.	MISC	edover
HackerOne	MISC	hacker
CVE Program record	CVE.ORG	www.c
NVD vulnerability detail	NVD	nvd.nis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)